



Análisis de la aplicación *CoronApp*

Informe sintético de análisis técnico

Este informe se basa en investigaciones que se hicieron principalmente en las versiones 1.2.29, 1.2.30, 1.2.31 y 1.2.32 de CoronApp. Durante la investigación se encontraron nuevas versiones que han ido saliendo cada 3 o 4 días. No hay documentación de los cambios de versión que se realizaron.

Se envió una versión previa de este informe a las entidades del Gobierno involucradas en el desarollo y la implementación de esta aplicación, y se envió igualmente al COLCERT. Varios cambios se hicieron, tomando en cuenta algunos hallazgos del informe. Al día de esta publicación, la versión vigente de la aplicación es la 1.2.36. Algunos comentarios en itálica mencionan los cambios que se han hecho desde entonces.

Aunque se hayan corregido, el detalle de las vulnerabilidades que hemos encontrado no se publica aquí.

El objetivo de este ejercicio es contribuir a un mejoramiento de la seguridad digital y la privacidad.





0. Metodología

Además del examen de la información pública sobre *CoronApp*, que aparece en la aplicación misma y en la tienda *Google Play Store*, se usaron los siguientes métodos no intrusivos:

- análisis estático con las aplicaciones *Exodus Privacy*[1] y *ClassyShark 3xodus*[2] de los permisos de la aplicación y de los rastreadores presentes en el código fuente;
- análisis estático del código fuente legible de la aplicación con *Apktool*[3] y análisis del manifesto de la app (*Android Manifest*);
- análisis de los flujos de datos generados y recibidos por la aplicación instalada en un teléfono con Android 7 – en uso normal incluyendo el envió de datos a través de los formularios de registro y reporte de salud - con el programa *Wireshark*[4];
- análisis de tráfico pasivo usando máquinas virtuales y *Burp Suite*[5]*;* Burp es una herramienta de análisis de tráfico a través de un proxy HTTP que permite analizar los paquetes de datos del lado del cliente incluyendo los datos que van por SSL (HTTPS).

Nota1: Todavía no se ha podido hacer un análisis concienzudo a través de la herramienta Burp toda vez que las dos ultimas versiones analizadas de la app no corren en máquinas virtuales (al parecer solo corren en equipos con procesadores arm64).

Nota2: Antes de hacer los análisis que implicaran llenar formularios, se envió un correo electrónico a varias personas que pudieran tener que ver con la aplicación (del INS, de la AND y del MINTIC, ver Anexo [0]) para intentar asegurarnos que identificarían los formularios y no considerarían esa información dentro de los análisis que hagan y las alertas que pudieran generar en su sistema.

---

1 https://exodus-privacy.eu.org/en/
2 https://f-droid.org/en/packages/com.oF2pks.classyshark3xodus/
3 https://ibotpeaches.github.io/Apktool/
4 https://www.wireshark.org/ Para hacer esta captura, generamos un punto de acceso WIFI desde el computador que ejecutaba el programa WireShark. El teléfono con la aplicación CoronApp accedía a Internet a través de este punto WIFI.
5 https://portswigger.net/





1. Datos colectados por la aplicación

La aplicación colecta los siguientes datos (ver pantallazos en Anexo [1]):

Tipo de datos	Datos
Datos personales del formulario de registro	• nombre y apellido • tipo y número de documento • celular • sexo • fecha de nacimiento • país, departamento, ciudad de residencia • correo electrónico • contraseña
Datos personales sensibles de los formularios de reporte y de inscripción	• origen étnico • reporte de salud: estoy bien / estoy mal • síntomas • contacto con personas con síntomas • atención médica recibida • viaje a otros países
Datos susceptibles de ser colectados por la aplicación de manera "no visible"	• contactos del teléfono • localización del dispositivo (enviado sistemáticamente por la app[6]) • redes WIFI cercanas • información disponible vía Bluetooth, en particular sobre otros dispositivos Bluetooth cercanos

La última parte tiene que ver con las autorizaciones amplias que solicita la aplicación.

En las últimas versiones, se redujeron los datos que recogen en el formulario de registro, limitándolos a: nombre y apellido, tipo y número de documento, número de teléfono celular.

6 Las coordenadas GPS aparecen en las capturas hechas con WireShark.





2. Permisos de la aplicación y colecta de datos pasiva

2.1 Permisos de la aplicación

La aplicación pide muchos permisos[7]. El siguiente es el listado que aparece cuando se utiliza *Exodus Privacy*. Estos coinciden con el manifiesto de la aplicación, ver anexo [2]):

24% 16:53
Exodus Privacy
19 Permissions
We have found the following permissions in the application:
MAPS_RECEIVE
INTERNET
tener acceso completo a la red
ACCESS_NETWORK_STATE
ver conexiones de red
ACCESS_COARSE_LOCATION
acceder a tu ubicación aproximada (basada en red)
ACCESS_FINE_LOCATION
acceder a tu ubicación precisa (basada en red y GPS)
READ_CONTACTS
consultar tus contactos
RECEIVE_BOOT_COMPLETED
ejecutarse al inicio

24% 16:53
Exodus Privacy
WAKE_LOCK
impedir que el teléfono entre en modo de suspensión
SET_ALARM
establecer una alarma
FOREGROUND_SERVICE
CALL_PHONE
llamar directamente a números de teléfono
READ_PHONE_STATE
consultar la identidad y el estado del teléfono
BLUETOOTH
vincular con dispositivos Bluetooth
ACCESS_WIFI_STATE
ver conexiones Wi-Fi
CHANGE_WIFI_STATE
conectarse a redes Wi-Fi y desconectarse

BLUETOOTH_PRIVILEGED
android.permission.BLUETOOTH_PRIVILEGED
BLUETOOTH_ADMIN
acceder a los ajustes de Bluetooth
RECEIVE
recibir datos de Internet
BIND_GET_INSTALL_REFERRER_SERVICE
API Install Referrer de Play
The icon ! indicates a 'Dangerous' or 'Special' level according to Google's protection levels.
Permissions are actions the application can do

Hay varios permisos que pueden ser intrusivos en cuanto a la privacidad:

- acceso a la localización: el análisis de las capturas con WireShark muestra que la aplicación enviá regularmente las coordenadas GPS del dispositivo;
- acceso a los contactos;
- acceso a la información de las redes WIFI disponibles que ve el dispositivo;
- acceso a los dispositivos Bluetooth que ve el teléfono.

Además una vez instalada, la aplicación se ejecuta sola al inicio (permiso “RECEIVE_BOOT_COMPLETED”).

Es importante resaltar que en la versión 1.2.29 de la aplicación se usaba sólo 14 permisos. Estos permisos se ampliaron a 19 a partir de la versión 1.2.30 y se mantienen en las versiones siguientes analizadas. Los tres permisos vinculados con Bluetooth son

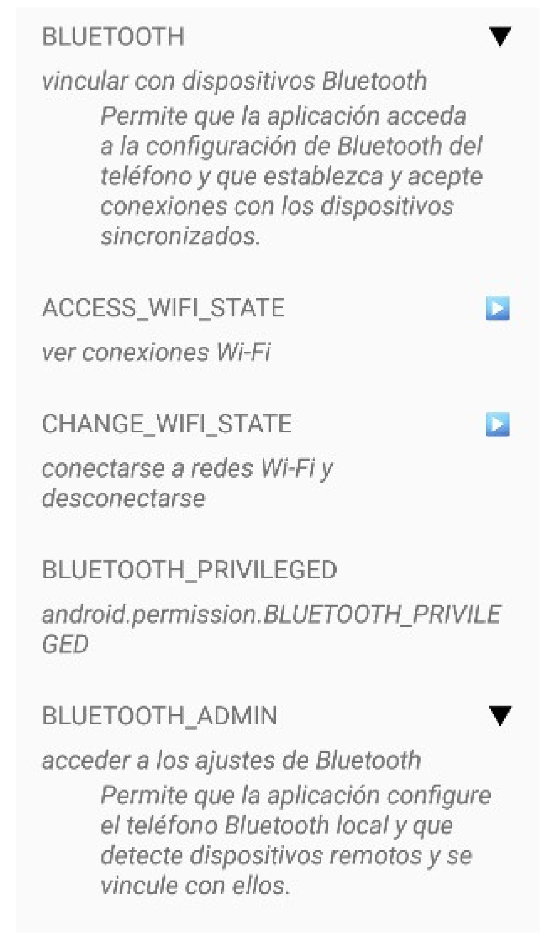
7 La mayoría no se piden explícitamente al usuario durante su instalación o su uso.





nuevos y no encontramos una explicación o información al respecto en la documentación de la aplicación.

Como lo muestra el pantallazo siguiente, el permiso BLUETOOTH_ADMIN puede ser bastante intrusivo ya que puede detectar los dispositivos cercanos (con el Bluetooth activado).



En la última versión de la aplicación, hay 16 permisos. Se ha quitado el de acceso a los contactos. Los permisos vínculados acceso a la localización, al Bluettoth y a las redes WIFI cercanas siguen.





2.2 Una curiosidad: la inclusión de la librería HypeLabs en las últimas versiones de la aplicación

En el manifiesto Android de la aplicación se muestra la inclusión del kit de desarollo de software (SDK) llamado “Hypelabs”[8]. HypeLabs es una empresa que desarrolla este SDK para dar a las aplicaciones habilidades de crear redes locales de tipo “mesh” usando los dispositivos de comunicación disponibles en el teléfono como Bluetooth y WiFi. Esto quizás se pueda conectar con los nuevos permisos de la aplicación que acabamos de mencionar.

CoronaApp introduce este SDK en la versión 1.2.30. Los pocos cambios introducidos en la versión 1.2.31 se refieren a esta misma librería. Causa curiosidad este cambio, ya que en la documentación publicada de esta aplicación nunca se menciona una característica de la App que requiera esta funcionalidad. Sin embargo, esta librería facilitaría, en combinación con el uso de los datos personales que recoge la aplicación, deducir la ubicación relativa de una persona con otra. Las conclusiones éticas y legales de este tipo de vigilancia deben ser revisadas si esta hipótesis se llegara a confirmar.

Es importante anotar que no se ha llegado a la conclusión de que este sea el uso que se le va a dar las capacidades de esta librería. De hecho, la aplicación no estaba haciendo uso de esta librería hasta la última versión.

Son necesarios más análisis para arrojar una respuesta concluyente a este caso.

Tanto para las autorizaciones mencionadas cómo para la inclusión, de esta biblioteca, la Agencia Nacional Digital nos respondió lo siguiente:

> *“La solicitud de los permisos de geolocalización, redes WiFi y Bluetooth, así como el tratamiento de dichos datos, son necesarios para identificar la localización de los usuarios y el contacto cercano que éstos puedan tener con personas a su alrededor, toda vez que permitirá localizar a los ciudadanos con potenciales síntomas, posibles focos y cadenas de contagio del COVID-19, permitiendo al Instituto Nacional de Salud recopilar la información necesaria y oportuna para actuar con diligencia ante los grandes riesgos de propagación identificados en la población.”*

8 https://hypelabs.io/





3. Seguridad de los envíos de datos de la aplicación

3.1 Un envío de datos no seguro hasta la versión 1.2.31

Hasta la versión 1.2.31 de la aplicación, los análisis de los flujos generados por la aplicación desde el teléfono (Wireshark) o desde un entorno de emulación (Burp) mostraban que los datos personales de registro eran enviados sin seguridad y sin cifrado, con el protocolo HTTP[9]. El envío se hacia a un sub dominio dedicado de la Agencia Nacional Digital del Gobierno ("apicovid.and.gov.co"), en un servidor web de *Amazon Web Services*, en el Estado de Washington[10] (ver Anexo [3]). El servidor web es un servidor Nginx versión 1.17.9 (última versión).

El análisis muestra también que las coordenadas GPS del dispositivo se envián regularmente a este mismo servidor y con el mismo protocolo.

En cuanto a los envíos de datos de salud (reportes), no se había podido identificar con certeza los paquetes que la transmiten porque la información está codificada, ya que se trataba de casillas que hay que marcar. Sin embargo, ya que al momento del envió de estos datos, la aplicación se comunicaba únicamente con el protocolo HTTP (hacia un servidor con la misma dirección IP), se puede deducir – con casi certeza – que el envió de datos no era seguro tampoco.

A partir de la versión 1.2.32 (del 31 de marzo) se remplazó el uso del protocolo HTTP por el protocolo seguro HTTPS (HTTP encapsulado en en el protocolo cifrado SSL/TLS). Se creó un nuevo subdominio "apicovid2.and.gov.co") asociado a un nuevo servidor web[11], con el cual la aplicación se comunica ahora.

Esta es una mejora importante en cuanto a la seguridad de la aplicación ya que los datos ahora son enviados en una forma cifrada.

Sin embargo la vulnerabilidad seguramente sigue en los equipos de las personas que no han actualizado la aplicación ya que el antiguo servidor sigue activo y se siguen enviando datos a él de forma no segura. Además unos análisis complementarios hechos por la linea de atención de la ONG Access Now, mostraron que el nuevo servidor seguía respondiendo al protocolo HTTP con el protocolo HTTP.

Esto se corrigió y en las últimas versiones, se cerró definitivamente la posibilidad que la aplicación se comunicara con el servidor con el protocolo HTTP.

9 *HyperText Transfer Protocol*. El envío se hace con un puerto inusual (5000) pero esto no cambia la ausencia de seguridad del protocolo.
10 El servidor web tiene la dirección IP: 52.87.234.39.
11 El nuevo servidor

3.2 Una vulnerabilidad grave en la autenticación de la aplicación

[Aunque la vulnerabilidad mencionada en esta parte ha sido aparentemente corregida, hemos quitado algunos detalles aquí, con el objetivo no facilitar ataques. El objetivo de este ejercicio es contribuir a un mejoramiento de la seguridad digital y la privacidad.]

Esta vulnerabilidad tiene que ver con un defecto de autenticación y podría permitir a un atacante acceder a datos personales de usuarios registrados en el servidor “backend” de la aplicación (con el cual se comunica la aplicación).

El servidor “backend” de *Coronapp_colombia* no hace suficiente control de acceso a recursos que deberían estar restringidos para cada usuario, ocasionando que un atacante tenga la habilidad de acceder a recursos de usuarios sin necesidad de ninguna autenticación. Esta vulnerabilidad podría provocar una posible enumeración de muchos datos sensibles de usuarios registrados en la aplicación.

En una revisión de paquetes hecha en el flujo de la aplicación, se encontró que algunos paquetes que deberían llevar un token de autenticación no lo llevan y no obstante la API despacha respuestas que corresponden a acciones que normalmente deberían llevar autenticación.

Este error se encuentra en el servidor que se venía usando hasta la versión 1.2.31 de la aplicación (servidor http sin SSL/TLS, dominio "apicovid.and.gov.co" y dirección IP:52.87.234.39”) y que al parecer fue reemplazado en la versión 1.2.32 como se acaba de mencionar (servidor http con ssl, dominio “apicovid2.and.gov.co” y dirección IP: 34.199.57.23). Sin embargo el servidor original no ha salido de funcionamiento y hace la vulnerabilidad posible.

[...]

Teniendo esto en cuenta, es probable que otros “endpoints” (URL) de la aplicación tengan el mismo problema. [...]

lo cual facilitaría automatizar el ataque para extraer información.

Pensamos que la vulnerabilidad se puede reproducir haciendo una solicitud a la api alojada en:

[...]

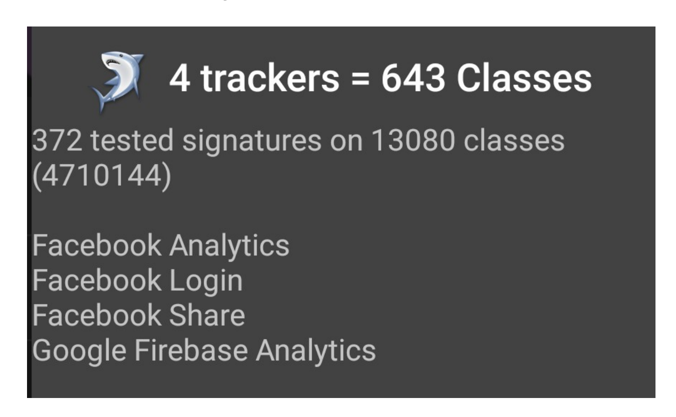
Para efectos de evaluar nuestro hallazgo pedimos a la línea de atención a incidentes de seguridad de la ONG *Access Now* revisar nuestro diagnóstico sobre esta vulnerabiliadd y ellos están de acuerdo con nuestro análisis.





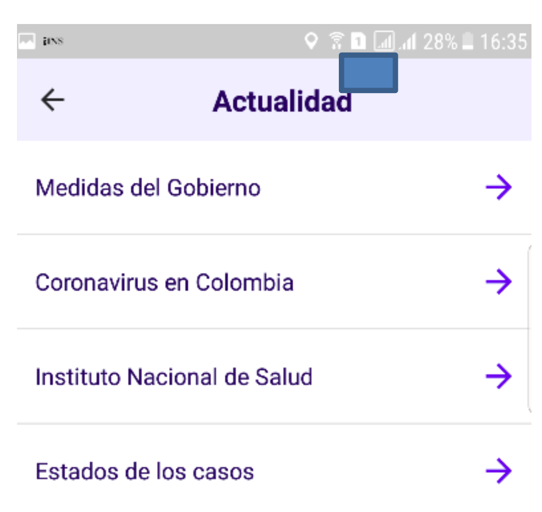
4. Rastreadores en la aplicación

El análisis de los rastreadores presentes directamente en el código de la aplicación nos muestra los siguientes (los mismos aparecen en la versión 1.2.31):



La consecuencia de su utilización es que se pueden observar conexiones con los servidores de Google y de Facebook en las capturas de flujo (Wireshark). Esto genera obviamente un rastreo del usuario por estos terceros actores en el uso de una aplicación sensible en cuanto a los datos que trata.

Hay que resaltar también que en relación con la función informativa de la aplicación, esta se conecta con los sitios de Presidencia, del Instituto Nacional de Salud, y del Ministerio de Salud. Aparecen conexiones con varios servidores de terceros, incluyendo actores publicitarios:



Sin embargo la presencia de estos últimos no se debe directamente a la aplicación sino a los sitios Internet externos de los cuales extraen la información.

En la última versión de la aplicación, hay dos rastreadores (Google CrashLytics y *Google Firebase Analytics). Se han quitado los de Facebook.*





ANEXOS – Referencias

[0] Correo preliminar enviado al INS, a la AND y al MINTIC

Asunto:	Análisis de la aplicación CoronApp
Fecha:	Sat, 28 Mar 2020 15:35:43 -0500
De:	XXXXXX - Karisma <XXXXXXX@karisma.org.co>
Organización:	Fundación Karisma
Para:	XXX@ins.gov.co, XXX@mintic.gov.co, XXX@and.gov.co, XXX@mintic.gov.co
CC:	XXX XXX <XXXX@karisma.org.co>, XXX XXX<XXXXX@karisma.org.co>

Buenas tardes,

La Fundación Karisma es una organización de la sociedad civil, fundada en 2003 y localizada en Bogotá, que busca responder a las oportunidades y amenazas que surgen en el contexto de la "tecnología para el desarrollo" para el ejercicio de los derechos humanos. Karisma trabaja desde el activismo con múltiples miradas —legales y tecnológicas— en coaliciones con socios locales, regionales e internacionales.

Desde hace varios años estamos evaluando aspectos de seguridad y privacidad de algunas páginas web y aplicaciones asociadas con trámites y servicios de interés público. Estos análisis han sido de conocimiento del Ministerio de Tecnologías (MINTIC) que en varias ocasiones nos ha facilitado mecanismos de comunicación con los responsables de las plataformas evaluadas. Esperamos que este sea nuevamente el caso.

En este momento **estamos haciendo un análisis no intrusivo de la aplicación CoronApp**, impulsada por el Instituto Nacional de Salud, en estos aspectos de privacidad y seguridad digital. Parte de nuestra evaluación incluye el análisis del tráfico de datos generado por los formularios que recopilan información personal, y por esto, queremos comunicarles que encontrarán registros a nombre de Karisma, asociados al correo XXX@karisma.org.co. Estos datos no son reales y no deben ser tomados en cuenta para los reportes de salud ni la generación de alertas.

Una vez tengamos el informe de nuestros hallazgos sobre la aplicación CoronApp los daremos a conocer en primera instancia a ustedes.

Si tienen alguna duda o inquietud sobre el tema pueden comunicarse con nosotros respondiendo este correo. Estaremos atentos a contestar cualquier pregunta.

Atentamente,

Fundación Karisma.





[1] Formularios de colecta de datos de la aplicación CoronApp

(como completados para el análisis)

20% 17:18	19% 17:21
Registro	**Registro**
Nombres: Fundacion Karisma	Fecha de nacimiento: 01/01/1940
Apellidos: TestNotomarEnCuenta	País de residencia: Colombia
Tipo de documento: Cédula de Ciudadanía	Departamento: Bogota D.C.
Número de documento: 1234567890	Ciudad: Bogota
Celular: 3123456789	Pertenencia étnica (opcional): Negro, mulato o afrodescendiente
Sexo: Mujer	Correo electrónico: test@karisma.org.co
Fecha de nacimiento	Contraseña: ••••••••





17% 17:37

Síntomas

¿Cómo te sientes hoy 28 de marzo?

Conocer tu estado de salud nos permite prevenir la propagación del Coronavirus.

Me siento bien

Me siento mal

Estaremos pendientes de tu salud

Cuéntanos cuáles son tus síntomas para orientarte

16% 17:38

Reporte de síntomas

¿Qué síntomas tienes hoy?

- Congestión nasal
- Dificultad para respirar
- Dolor de garganta
- Dolor de músculos
- Escalofrío
- Fatiga
- Fiebre
- Malestar

16% 17:39

Reporte de síntomas

- Malestar
- Tos
- ¿Está en autoaislamiento?

En los últimos 14 días...

- ¿Has estado con alguna persona con síntomas similares?
- ¿Has recibido atención médica?
- ¿Has estado en otro país?

REPORTAR




[2] Permisos de la aplicación. El manifiesto de la aplicación en *AndroidManifest*

(*Android Manifest*, archivo .xml hecho por los desarrolladores para describir la aplicación técnicamente)

AndroidManifest.xml (~/karisma/coronapp/co.gov.ins.guardianes_33_apps.evozi.com)

File Edit View Search Tools Documents Help


```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="29"
android:compileSdkVersionCodename="10" package="co.gov.ins.guardianes" platformBuildVersionCode="29" platformBuildVersionName="10">
    <uses-permission android:name="co.gov.ins.guardianes.permission.MAPS_RECEIVE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="com.android.alarm.permission.SET_ALARM"/>
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
    <uses-feature android:name="android.hardware.bluetooth_le" android:required="true"/>
    <uses-permission android:name="android.permission.BLUETOOTH_PRIVILEGED"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>
    <uses-feature android:name="android.hardware.camera" android:required="true"/>
    <uses-feature android:glEsVersion="0x00020000" android:required="true"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
    <application android:allowBackup="true" android:appComponentFactory="androidx.core.app.CoreComponentFactory" android:extractNativeLibs="false" android:icon="@mipmap/
ic_gds" android:isSplitRequired="true" android:label="@string/app_name_short" android:largeHeap="true" android:name="co.gov.ins.guardianes.manager.Application"
android:roundIcon="@mipmap/ic_gds" android:theme="@style/Theme.Home" android:usesCleartextTraffic="true" android:networkSecurityConfig="@xml/network_security_config">
        <activity android:exported="false" android:name="co.gov.ins.guardianes.view.menu.CoronappAbout"
android:parentActivityName="co.gov.ins.guardianes.view.HomeActivity" android:screenOrientation="portrait" android:theme="@style/Theme.NoActionBar"/>
        <activity android:name="co.gov.ins.guardianes.view.news.TypeOfDiseaseActivity" android:parentActivityName="co.gov.ins.guardianes.view.news.NewsActivity"
android:screenOrientation="portrait" android:theme="@style/Theme.NoActionBar" android:usesCleartextTraffic="true"/>
        <activity android:name="co.gov.ins.guardianes.view.welcome.WelcomeIntro" android:screenOrientation="portrait"/>
        <uses-library android:name="org.apache.http.legacy" android:required="false"/>
        <activity android:name="co.gov.ins.guardianes.view.SplashActivity" android:noHistory="true" android:screenOrientation="fullSensor" android:theme="@style/
Theme.NoActionBar">
```





[3] Envió de los datos de Registro con el protocolo HTTP (versión 1.2.30)

```
Wireshark · Packet 535 · Captura WireShark 2 (Registro).pca
› Frame 535: 925 bytes on wire (7400 bits), 925 bytes captured (7400 bits) on interface 0
› Ethernet II, Src: MurataMa_18:e0:1f (b8:d7:af:18:e0:1f), Dst: klab-Inspiron-7559.local (84:ef:18:ce:6a:21)
› Internet Protocol Version 4, Src: 10.42.0.202 (10.42.0.202), Dst: apicovid.and.gov.co (52.87.234.39)
› Transmission Control Protocol, Src Port: 57220, Dst Port: 5000, Seq: 1, Ack: 1, Len: 859
˅ IPA protocol ip.access, type: unknown 0x53
    DataLen: 20559
    Protocol: Unknown (0x53)

0000  84 ef 18 ce 6a 21 b8 d7  af 18 e0 1f 08 00 45 00   ····j!·· ······E·
0010  03 8f 5f 52 40 00 40 06  ae a4 0a 2a 00 ca 34 57   ··_R@·@· ···*··4W
0020  ea 27 df 84 13 88 c6 a8  74 62 c1 10 4a 54 80 18   ·'······ tb··JT··
0030  02 ad 37 4e 00 00 01 01  08 0a 00 13 2b 3e 06 1e   ··7N···· ····+>··
0040  81 c5 50 4f 53 54 20 2f  75 73 65 72 2f 63 72 65   ··POST / user/cre
0050  61 74 65 20 48 54 54 50  2f 31 2e 31 0d 0a 61 70   ate HTTP /1.1··ap
0060  70 5f 74 6f 6b 65 6e 3a  20 64 34 31 64 38 63 64   p_token:  d41d8cd
0070  39 38 66 30 30 62 32 30  34 65 39 38 30 30 39 39   98f00b20 4e980099
0080  38 65 63 66 38 34 32 37  65 0d 0a 43 6f 6e 74 65   8ecf8427 e··Conte
0090  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61   nt-Type:  applica
00a0  74 69 6f 6e 2f 6a 73 6f  6e 0d 0a 43 6f 6e 74 65   tion/jso n··Conte
00b0  6e 74 2d 4c 65 6e 67 74  68 3a 20 36 32 36 0d 0a   nt-Lengt h: 626··
00c0  48 6f 73 74 3a 20 61 70  69 63 6f 76 69 64 2e 61   Host: ap icovid.a
00d0  6e 64 2e 67 6f 76 2e 63  6f 3a 35 30 30 30 0d 0a   nd.gov.c o:5000··
00e0  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 65 65 70   Connecti on: Keep
00f0  2d 41 6c 69 76 65 0d 0a  41 63 63 65 70 74 2d 45   -Alive·· Accept-E
0100  6e 63 6f 64 69 6e 67 3a  20 67 7a 69 70 0d 0a 55   ncoding:  gzip··U
0110  73 65 72 2d 41 67 65 6e  74 3a 20 6f 6b 68 74 74   ser-Agen t: okhtt
0120  70 2f 34 2e 32 2e 32 0d  0a 0d 0a 7b 22 66 69 72   p/4.2.2· ···{"fir
0130  73 74 6e 61 6d 65 22 3a  22 46 75 6e 64 61 63 69   stname": "Fundaci
0140  6f 6e 20 4b 61 72 69 73  6d 61 22 2c 22 6c 61 73   on Karis ma","las
0150  74 6e 61 6d 65 22 3a 22  54 65 73 74 4e 6f 74 6f   tname":" TestNoto
0160  6d 61 72 45 6e 43 75 65  6e 74 61 22 2c 22 64 6f   marEnCue nta","do
0170  63 75 6d 65 6e 74 5f 74  79 70 65 22 3a 22 43 43   cument_t ype":"CC
0180  22 2c 22 64 6f 63 75 6d  65 6e 74 5f 6e 75 6d 62   ","docum ent_numb
0190  65 72 22 3a 22 31 32 33  34 35 36 37 38 39 30 22   er":"123 4567890"
01a0  2c 22 70 68 6f 6e 65 22  3a 22 33 31 32 33 34 35   ,"phone" :"312345
01b0  36 37 38 39 22 2c 22 65  6d 61 69 6c 22 3a 22 74   6789","e mail":"t
01c0  65 73 74 40 6b 61 72 69  73 6d 61 2e 6f 72 67 2e   est@kari sma.org.
01d0  63 6f 22 2c 22 70 61 73  73 77 6f 72 64 22 3a 22   co","pas sword":"
01e0  41 7a 65 72 74 79 37 38  22 2c 22 63 6c 69 65 6e   Azerty78 ","clien
01f0  74 22 3a 22 61 70 69 22  2c 22 67 65 6e 64 65 72   t":"api" ,"gender
0200  22 3a 22 46 65 6d 65 6e  69 6e 6f 22 2c 22 61 70   ":"Femen ino","ap
0210  70 5f 74 6f 6b 65 6e 22  3a 22 64 34 31 64 38 63   p_token" :"d41d8c
```

Aquí se puede ver un paquete HTTP enviando los datos del formulario. El uso inusual del puerto 5000 hace que Wireshark no reconozca el protocolo HTTP, pero su contenido muestra que sí lo es (*POST /user/create HTTP /1.1*) y muestra los datos llenados en el formulario de registro: firstname: Fundacion Karisma, lastname: TestNoTenerEncuenta, document number 1234567890, phone: 3123456789, email: test@karisma.org.co, gender: femenino e incluso el password: Azerty78. En la parte que sigue aparecen también todos los otros datos ingresados en el formulario.

El envió se hace hacia el dominio “apicovid.and.gov.co” en un servidor con dirección IP 52.87.234.39.





[4] Este Anexo se ha quitado.

Con el objetivo de no facilitar ataques, aun cuando sabemos que la vulnerabilidad reportada está en este momento parchada, no divulgaremos los detalles de este anexo.
El objetivo de este ejercicio es contribuir a un mejoramiento de la seguridad digital y la privacidad.





[5] Extracto de capturas con Wiresark, versión 1.2.31 de la app ejecutada en un teléfono Android 7

Con el objetivo de no facilitar ataques, aun cuando sabemos que la vulnerabilidad reportada está en este momento parchada, se ha quitado una sección de este anexo (la solicitud). Sin embargo se deja aquí una parte de la respuesta del servidor que muestra los datos personales a los que se tenía acceso.

HTTP/1.1 200 OK
Server: nginx/1.17.9
Date: Mon, 30 Mar 2020 00:04:43 GMT
Content-Type: application/json; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
25a
{"error":false,"message":[...]","member":{"id":[...]","picture":0,"dob":"1942-01-01T00:00:00","city":"Bogota","state":"Bogota D.C.","gender":"Hombre","firstname":"Fundacion Karisma dos","user":"[...]","platform":"android","client":"api","country":"Colombia","race":"Indigena","relationship": "Conyugue","lastname":"PruebaNotomarEncuentaEstosDato","app_token":"d41d8cd98f00b204e9800998ecf8427e","createdAt":"2020-03-30T00:04:43.2472659+00:00", "updatedAt":"2020-03-30T00:04:43.2472702+00:00","document_number":"1234567899","document_type":"TI"}}





[6] Extracto de flujo con Burp Burp (versión de la app 1.2.29)

En este anexo también se prensenta sólo una parte del Anexo original (la respuesta del servidor).

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.17.9
Date: Tue, 31 Mar 2020 20:47:39 GMT
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 2361
```


```
{"error":"false","data":[{"surveys":[{"id":"5e83a9f9ebc6fc0001072d67","platform":"android","no_symptom":"Y","lon":-122.084,"lat":37.4219983,"app_token":
"d41d8cd98f00b204e9800998ecf8427e","user":"5e83a9e0ebc6fc0001072d65","week_of":"2020-03-31T20:37:13.866Z","coordinates":[-122.084,37.4219983],"createdAt":
"2020-03-31T20:37:13.866Z","updatedAt":"2020-03-31T20:37:13.866Z","client":"api","hadTravelledAbroad":false,"startDate":"0001-01-01T00:00:00Z","hadContagiousContact":false,
"hadHealthCare":false},{"id":"5e83a9f9ebc6fc0001072d66","platform":"android","no_symptom":"Y","lon":-122.084,"lat":37.4219983,"app_token":"d41d8cd98f00b204e9800998ecf8427e",
"user":"5e83a9e0ebc6fc0001072d65","week_of":"2020-03-31T20:37:13.858Z","coordinates":[-122.084,37.4219983],"createdAt":"2020-03-31T20:37:13.858Z","updatedAt":
"2020-03-31T20:37:13.858Z","client":"api","hadTravelledAbroad":false,"startDate":"0001-01-01T00:00:00Z","hadContagiousContact":false,"hadHealthCare":false}],"user":{"id":
"5e83a9e0ebc6fc0001072d65","picture":0,"dob":"1900-01-01T00:00:00Z","city":"Bogota","email":"test2@karisma.org.co","state":"Bogota D.C.","gender":"Masculino","firstname":
"usuario prueba","platform":"android","country":"Colombia","race":"Escoge una opción","gcm_token":
"czwM3ujW-3E:APA91bHpXXOtwPhvtxOCnyc_28Ii74SSbfDwfTBU2fEy_JBA0YjHzosPOYmWifDN5P-fsaDAGzGSgM-lii69uVH4hyeWbA5XqsB8kwqqH4w1OegTQEchIH4lFY8yDyKP8cRpUVy9cwkT","lastname":"test",
"week_of":"2020-04-01T20:36:48.512Z","active":"Y","isAdmin":false,"app":"d41d8cd98f00b204e9800998","age":120,"ageGroup":"80","token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmlxdWVfbmFtZSI6IjVlODNhOWUwZWJjNmZjMDAwMTA3MmQ2NSIsIm5iZiI6MTU4NTY4NzAwOCwiZXhwIjoxNTg4Mjc5MDA4LCJpYXQiOjE1ODU2ODcwMDh9.UPE_NdBRtNqY
zAyLhxIPmN8RKoFAb3pmx-tFbwAMTJc","device_id":"4dc1b4eb13a5f495","document_number":"12345678","document_type":"CC","createdAt":"2020-03-31T20:36:48.512Z","updatedAt":
"2020-03-31T20:36:48.512Z"},"id":"5e83ac67ebc6fc0001072d80","picture":0,"dob":"1900-01-01T00:00:00Z","city":"Bogota","state":"Bogota D.C.","gender":"Hombre","firstname":
"usuario2 prueba","platform":"android","country":"Colombia","race":"Rom-Gitano","relationship":"Bisnieto","lastname":"test","appToken":"d41d8cd98f00b204e9800998ecf8427e",
"createdAt":"2020-03-31T20:47:35.982Z","updatedAt":"2020-03-31T20:47:35.982Z","documentNumber":"12345678","documentType":"CC"}]}
```